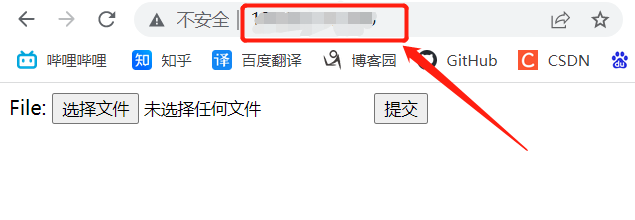
**一、靶场搭建**

1、Vulhub启动

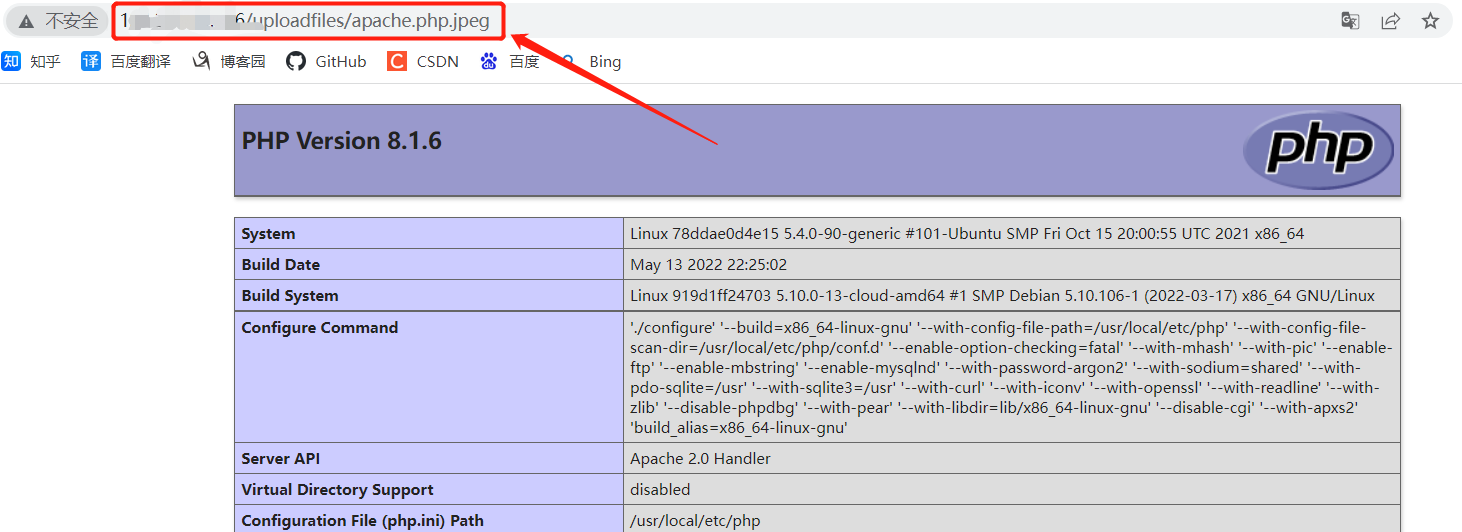
C:\Users\Toby\AppData\Local\Temp\1653551543(1).jpg

2、访问目标网址

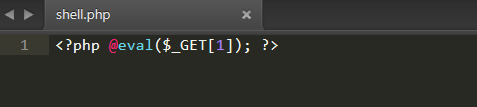


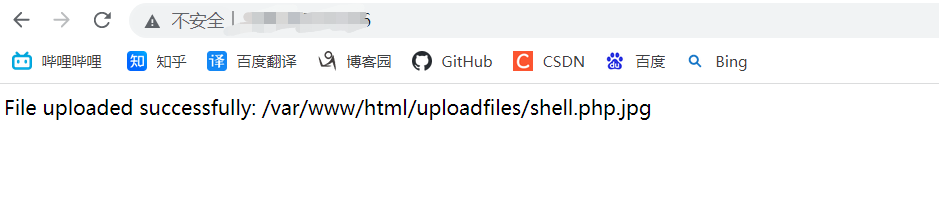
**二、漏洞复现**

1、访问/uploadfiles/apache.php.jpeg文件，发现phpinfo被成功执行，该文件被解析为php脚本



2、通过上传名为xxx.php.jpg或xxx.php.jpeg的文件，上传成功





3、访问该文件路径并传入命令

